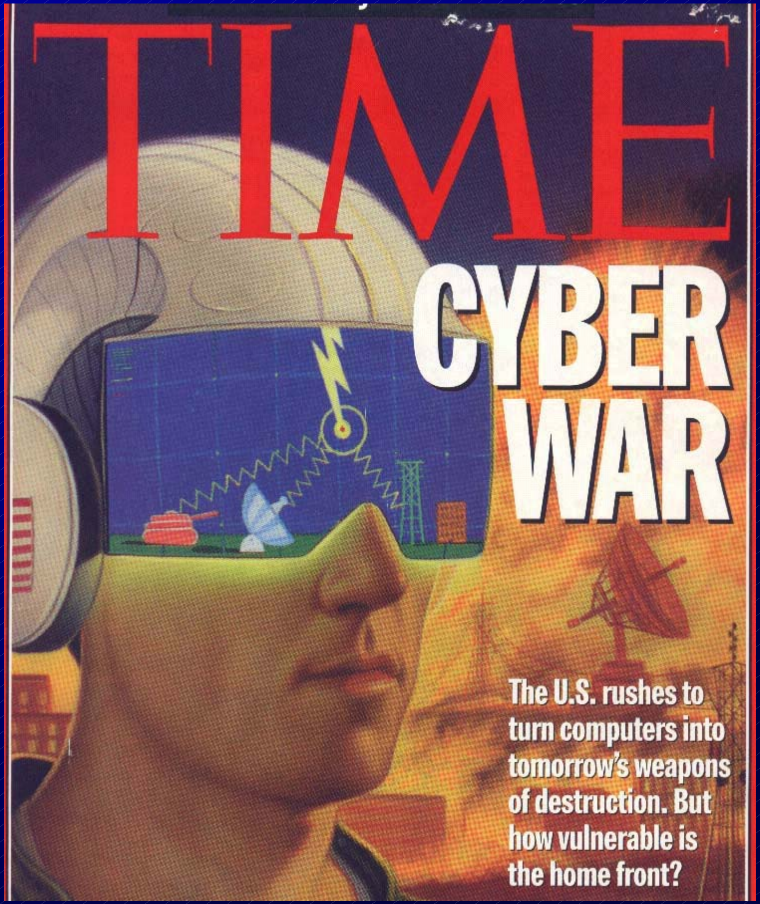

TIME
CYBER WAR
The U.S. rushes to turn computers into tomorrow's weapons of destruction. But how vulnerable is the home front?

Homeland Security

and

Information Operations

An Intro to

IO and IO legal issues

Commander James Bond, USN

Navy Judge Advocate General's Corps

International & Operational Law Division

"Which one of you is being held on computer hacking charges?"

IO -- Main Elements

- Electronic Warfare (EW)
- Psychological Operations (PSYOP)
- Operations Security (OPSEC)
- Military Deception (MILDEC)
- Civil Affairs (CA)
- Public Affairs (PA)
- Computer Network Exploitation/Attack (CNE/CNA)
- Computer Network Defense (CND)

What is Information Operations Law?

- No separate legal regime of “IO Law”
- Apply existing law to IO/IW activities, e.g.:
  - Law of Armed Conflict
  - Use of Force issues
  - Space Law
  - Intelligence Oversight
  - Telecommunications Law
  - Response to computer intrusions (CNR?)
- Operators & Lawyers are gaining more and more experience with IO legal issues (but still plenty of issues of first impression out there)

There are Two Aspects of the Legal Issues Surrounding IO

- What are the laws & policies affecting the use of IO in wartime, in operations other than war, and during peacetime operations, including any HLS role of DoD?
- How must the law evolve to strengthen U.S. interests, policies, and capabilities with regard to IO?

Information Dominance is an Important Part of HLS

"There's a war out there old friend, a world war, and it's not about who's got the most bullets. It's about who controls the information - about how we think, how we see and hear, how we work. *It's all about information. ..." Sneakers*

MCA Universal Pictures

1992

¬ *Explosion of Technology*

¬ *Lacк of Legal Guidance*

Example →

NSA has sole authority to conduct SIGINT per EO 12333. Issue: is defensive CNE SIGINT collection and can it be done by a Title 10 Authority.

DEFINITIONS

- **Information Operations (IO): Actions taken to affect adversary information and information systems while defending one's own information, and information systems. Includes both offensive and defensive IO.**
- **Information Warfare (IW): IO conducted during times of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.**
- **Information Assurance (IA): IO that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.**
- **Computer Network Attack (CNA): Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.**

DEFINITIONS (cont.)

- **Computer Network Defense (CND): Integrate and coordinate policies and procedures, operations, personnel and technology to protect and defend information and information systems.**
- **Information Superiority: The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying and adversary's ability to do the same.**
- **Information System: The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.**
- **Sensitive Information Operations: IO that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to national security of the U.S., require a special review and approval process**

IO -- Defensive or Offensive Use

OFFENSIVE INFORMATION OPERATIONS

"THE INTEGRATED USE OF ASSIGNED AND SUPPORTING CAPABILITIES AND ACTIVITIES, MUTUALLY SUPPORTED BY INTELLIGENCE, TO AFFECT ADVERSARY DECISION MAKERS TO ACHIEVE OR PROMOTE SPECIFIC OBJECTIVES."

DEFENSIVE INFORMATION OPERATIONS

"THE INTEGRATION AND COORDINATION OF POLICIES, PROCEDURES, OPERATIONS, PERSONNEL, AND TECHNOLOGY TO PROTECT AND DEFEND INFORMATION AND INFORMATION SYSTEMS"

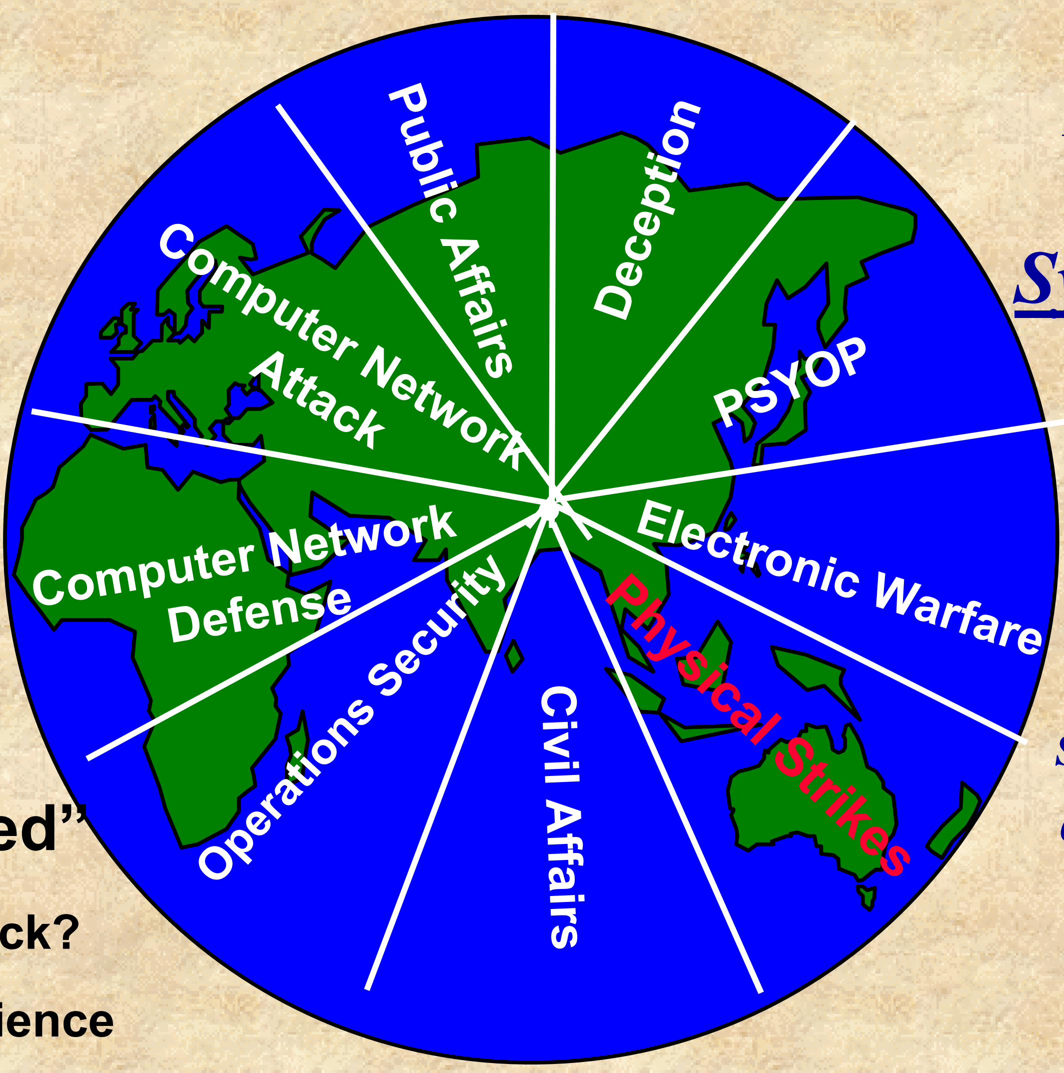
JOINT PUB 3-13

New Opportunities = New Vulnerabilities = New Legal Issues

(technically less difference; policy and legally a huge distinction)

Operationalizing IO

Effectively Conducting Information Operations means . . .



Integrating *and* ***Synchronizing*** *traditionally independent capabilities and activities in support of the commander's mission.*

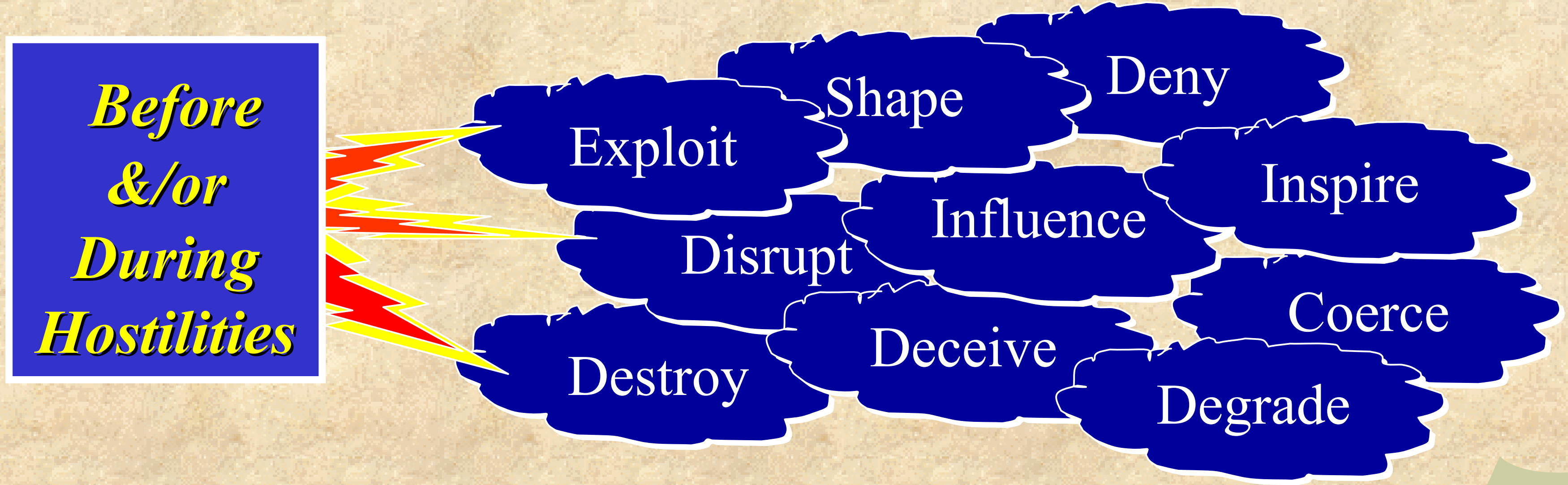
"Effects Based"

- Kinetic Attack?

- WWII Experience

IO -- What It Does

IO focuses on the opportunities (and vulnerabilities) presented by the increasing dependence of the U.S. and our potential enemies on information and information systems.



Before &/or During Hostilities

Exploit

Shape

Deny

Inspire

Influence

Disrupt

Coerce

Deceive

Destroy

Degrade

IO includes also Information Assurance

IO Target Areas

Asymmetric Ability to Affect Broad Spectrum of Target Areas

HUMAN FACTORS

LINKS

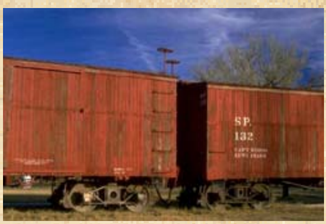
NODES

TROOPS

NATIONAL COMMAND AUTHORITIES

POPULACE

PROCESSORS

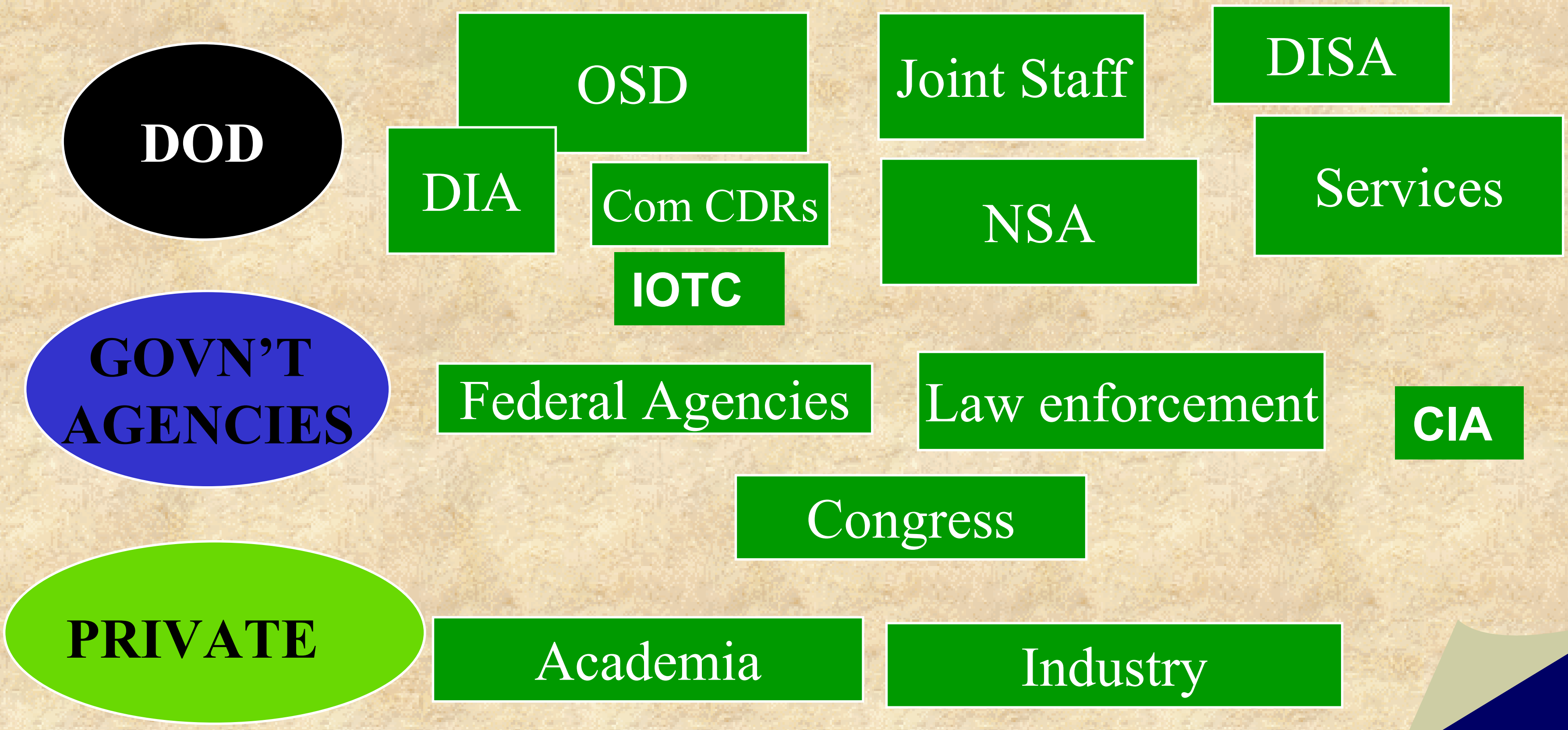


PHYSICAL PLANT

SATELLITES

IO COORDINATION in HLS

IO SUPPORTS THE NATIONAL MILITARY STRATEGY, BUT MUCH AUTHORITY/ RESPONSIBILITY FALLS OUTSIDE OF DoD



DOD

OSD

Joint Staff

DISA

DIA

Com CDRs

NSA

Services

IOTC

GOVN'T AGENCIES

Federal Agencies

Law enforcement

CIA

Congress

PRIVATE

Academia

Industry

The CND Challenge

- Why Does CND Matter?
- How Big Is The Problem?
- What Are We Doing About It?

"We are entering a period when one individual, or small groups of individuals, are able to wage war on our entire country. [Past] cyber attacks highlight the threat we face and to be brutally candid, I view hackers and crackers as the enemy and the insider hacker as a traitor in information warfare."

LTGEN William Donahue, quoting
Dr. John J. Hamre, Dep SECDEF.

CND vs. CNA

- U.S. military relies on its networks for:
  - Targeting
  - Command and Control
  - Support
  - *Most everything we do*
- Cyber attack offers asymmetric capability to:
  - Disrupt power, transportation, and communications
  - Destroy banking and financial records
  - Commit espionage remotely
  - *Degrade capability of military forces*

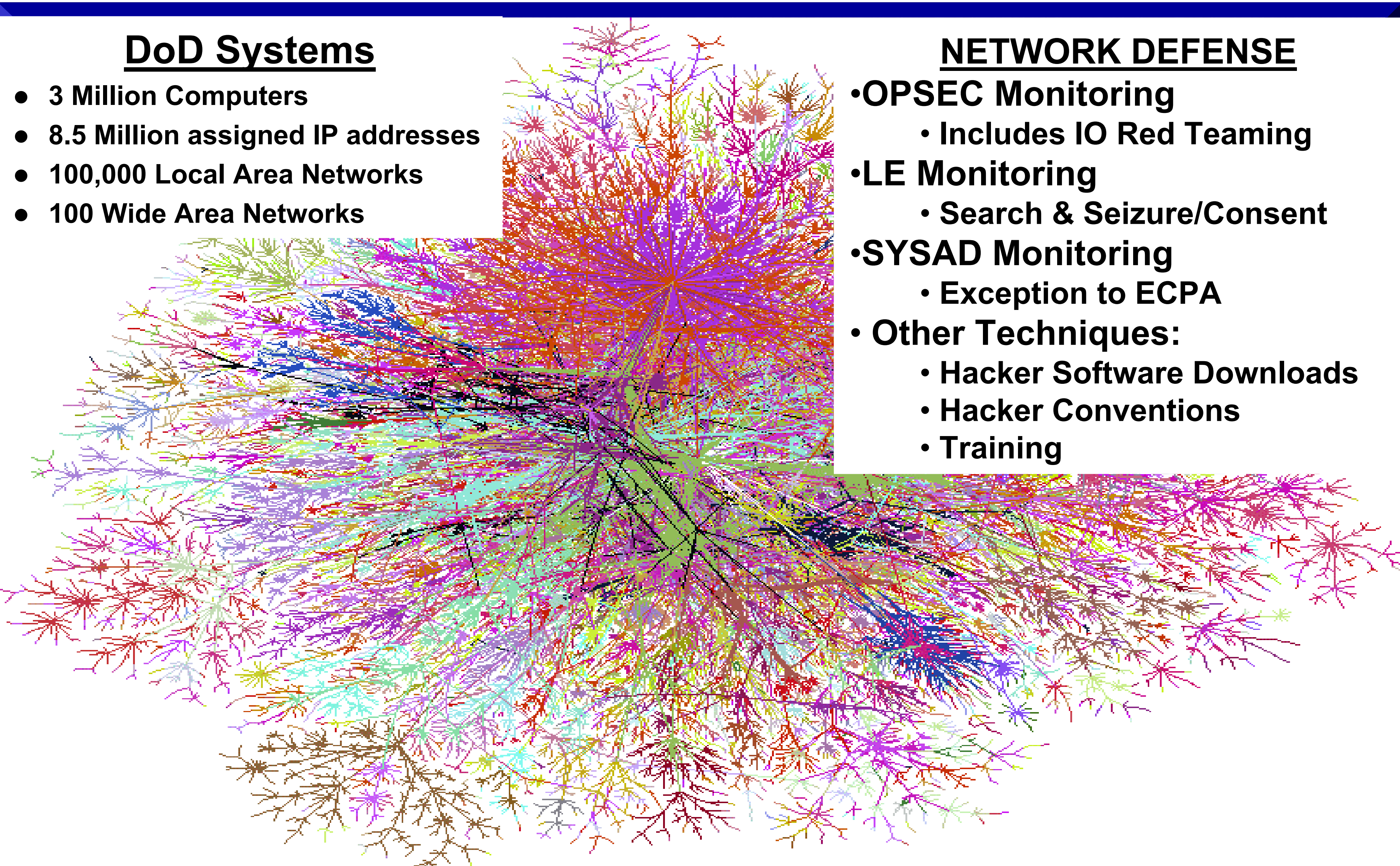
Computer Network Defense

DoD Systems

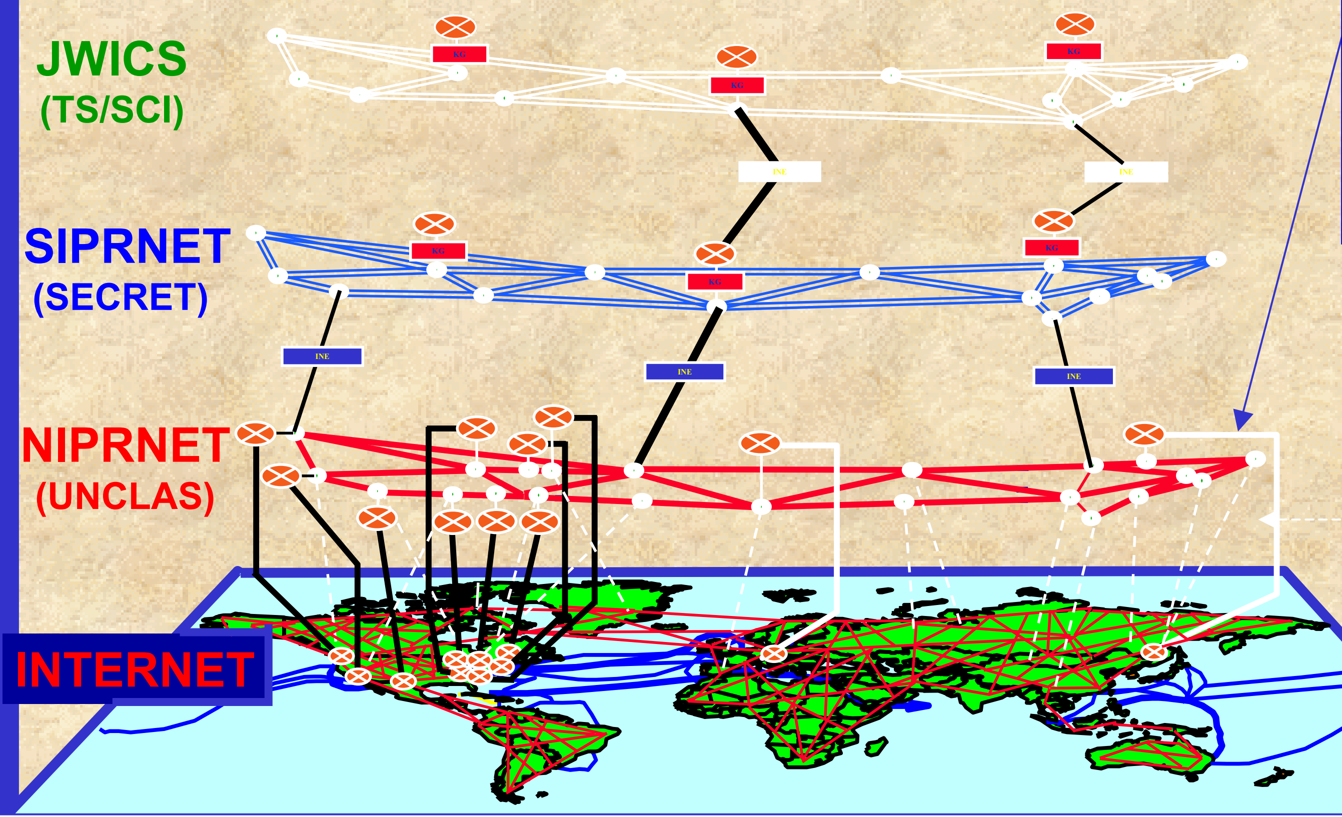
- 3 Million Computers
- 8.5 Million assigned IP addresses
- 100,000 Local Area Networks
- 100 Wide Area Networks

NETWORK DEFENSE

- OPSEC Monitoring
  - Includes IO Red Teaming
- LE Monitoring
  - Search & Seizure/Consent
- SYSAD Monitoring
  - Exception to ECPA
- Other Techniques:
  - Hacker Software Downloads
  - Hacker Conventions
  - Training



We Work Constantly to Protect Our Networks, but...



DISA Gateways

Positive Control
Protocol Filtering
Procedural Restrictions
Data Analysis Capability
Surge Capacity

Backdoors

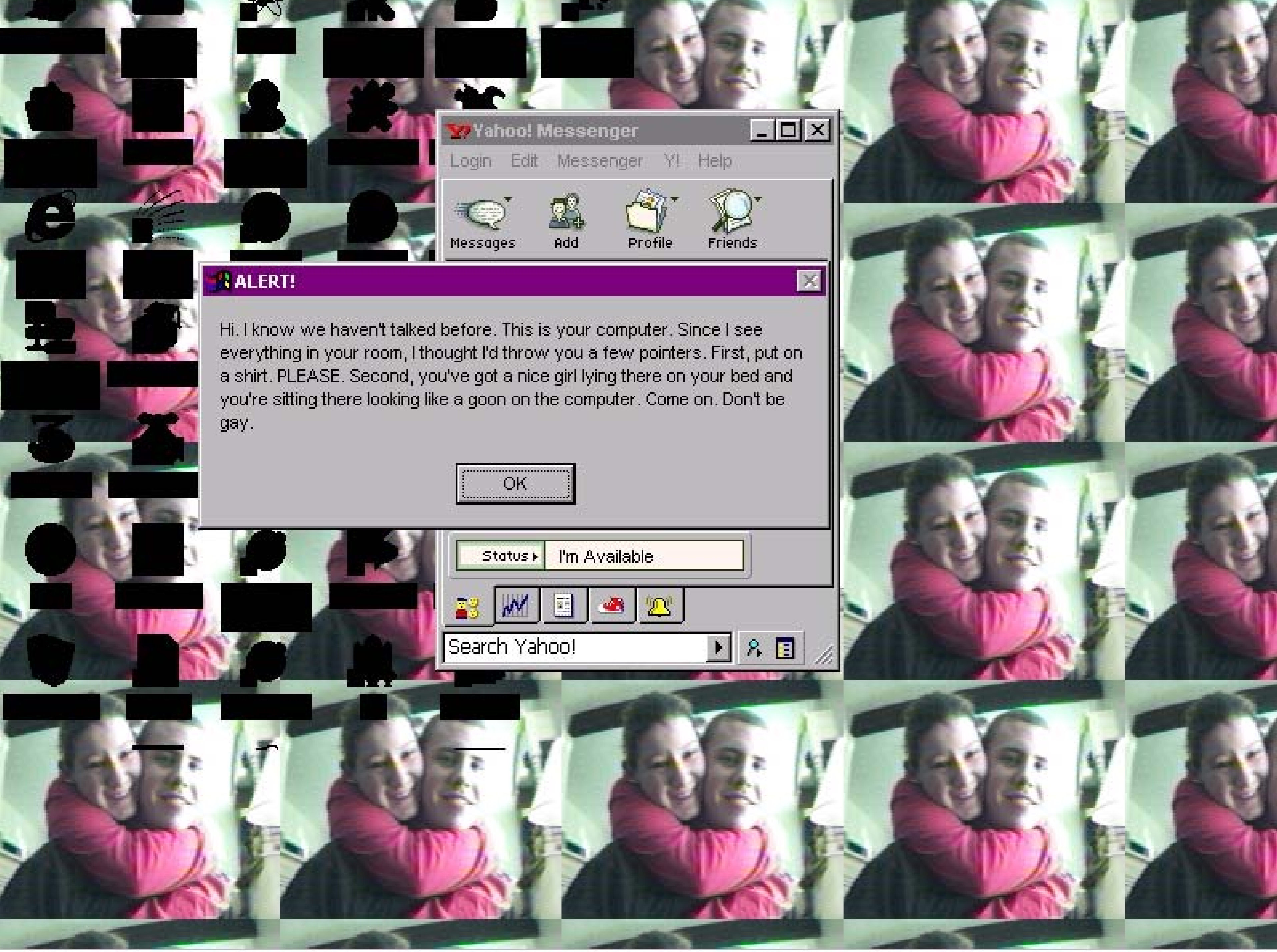
Many NIPRNET Backdoors
Reduced Security
No Control
No Filtering
No Restrictions

Interconnection = Utility = Vulnerability

Example of a System Intrusion

The following two screens demonstrate the ability of hackers to gain access into a computer or computer system and exercise control over that computer or computer system.

- **The first screen shows a pop-up message a hacker sent to a victim.**
- **The second screen shows the view from the victim's camera as he received the message.**



[redacted]

Hi. I know we haven't talked before. This is your computer. Since I see everything in your room, I thought I'd throw you a few pointers. First, put on a shirt. PLEASE. Second, you've got a nice girl lying there on your bed and you're sitting there looking like a goon on the computer. Come on. Don't be gay.

Status ▸ I'm Available

Time to call FIWC
at 1-888-NAVCIRT

The Cyber Attack Threats

Hacker

- Disgruntled Employee
- Industrial Espionage
- Foreign Espionage
- Terrorist
- State Sponsored Attack
- Insiders

There is serious debate whether we may be seeing only the tip of the iceberg or have things under control, but regardless, the threat is real and is increasing.

The Potential of the Threat

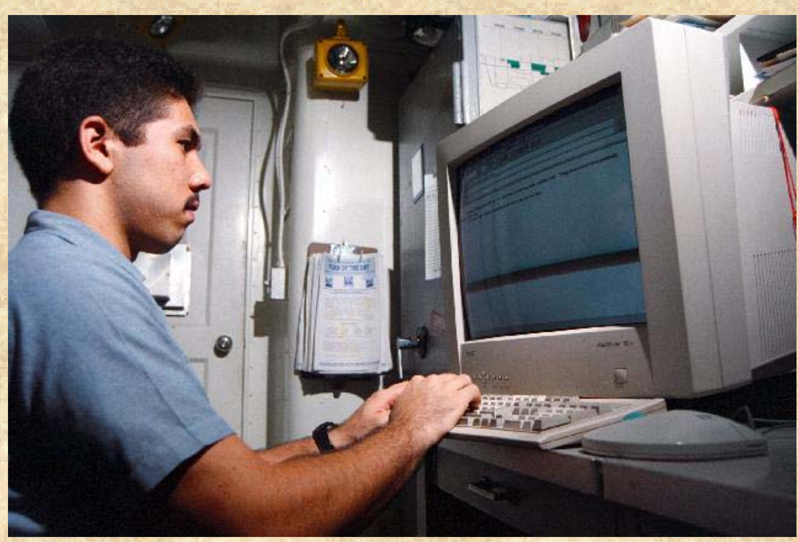
- 120 Countries or Groups with Computer Network Attack Capabilities
- 60-80 Cyber Attacks Daily on Navy Computer Systems
- 30,000 On-line Hacker Sites
- 17 Million Users with Sufficient Skills to be a Potential Hacker

Persistent intrusions onto DoD systems, code named Moonlight Maze

- *March 1998 to present*
- *James Adams in Foreign Affairs alleges critical data loss & "back doors" (Jun '01)*
- *CNE, not CNA*

Vulnerable but Improving

- ➢Internet was not Built to be Secure
- ➢COTS HW/SW Development Focused on "Slick, Stable, Simple" (not "Secure")
- ➢System Administrators Lack Training
- ➢User Awareness is Low



CND Exercise Eligible Receiver

-- June 1997

CND Exercise Zenith Star

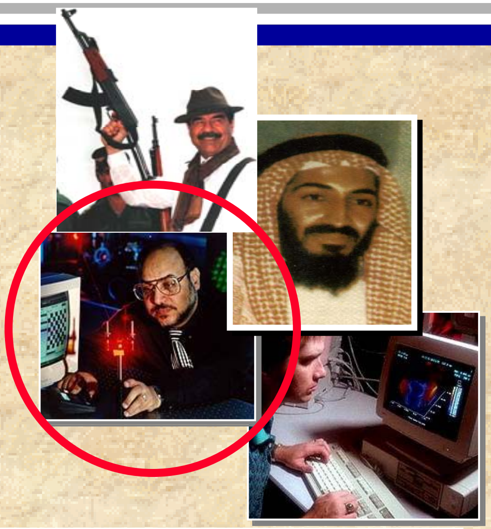
-- October 1999

eXtreme hacking

Defending Your Site

CND Technical Analysis Has both a Law Enforcement & Intel Side

Not Always Clear Which Set of Authorities to Proceed Under



Intelligence Authorities

- Foreign Intelligence Surveillance Act (50 U.S.C 1801, et.seq.)
- Exec Order 12333
- DODD 5240.1-R
- Agency Directives

Law enforcement processes may be only way to get information on US citizens

LE Authorities

- 4th Amendment (Monroe, Simons)
- Electronic Communication Privacy Act (18 U.S.C. 2510, et. seq.)
- Stored Communications (18 U.S.C. 2701, et. seq.)
- Pen Register, Trap and Trace (18 U.S.C. 3121, et. seq.)
- Computer Fraud and Abuse Act (18 U.S.C. 1030)
- Password Trafficking (18 U.S.C. 1029, 1030)
- Military Communication Systems (18 U.S.C. 1362)
- DOD O-5505.9-M Law Enforcement Electronic Intercepts

Summary on CND

- **Network size is weakness and strength**
  - Impossible to control and difficult to protect
  - Inherently resistant to widespread, operationally significant damage
- **Bad guy has tactical advantage**
  - Picks target, recons at no risk, chooses time of execution and operates under tolerant (or no) law and policy
  - We nearly always start late
  - We nearly always (initially) depend on law enforcement response
- **Most of our wounds are still self-inflicted**
- **We Have Made Tremendous Progress Since ER 97, But Are Still Vulnerable**

The DOJ Position

- "...unless an established predicate of international law has been met, the matter remains one for the law enforcement community... In most cases a lack of information will demand that we presume that
  - (1) the case is a criminal matter (as opposed to a national security case), and
  - (2) the hacker is protected by the Fourth Amendment as well as the laws of the United States…**[changed via Patriot Act?]**
- The Justice Department presumes not only that the hacker is protected by US laws, but that the criminal process should be used during the initial stages of the investigation"

- DOJ Letter to DOD, 11 Aug 99

IO & Intel Collection Are Closely Linked

Is CNE lawful espionage? Can CNE be a form of Self-Defense? In IO world, difference between espionage & attack can be line of computer code.

- **IO Cell questions during MOOTW in furtherance of HLS. What does the law permit :**
  - Mapping network as part of CNE/SIGINT Collection (non-intrusive collection)?
  - Assuring later access (e.g., trap doors) &/or latent malicious logic plants (intrusive collection)?
  - Disrupt, Deny, Degrade or Destroy data or info (very intrusive)?

Intelligence Law & HLS

"The necessity of procuring good intelligence is apparent and need not be further urged."

George Washington

- Challenging Area -- other SJA interface recommended
- Intel rules don't change even in emergency or special operation.

GW was probably our first Intel Case Officer.

Intel Oversight Program History

STEMMED FROM ABUSES DURING THE 60'S AND 70'S

- Pre-1970's Intel activities were assumed to be legal & congress gave great deference to President
- Rockefeller Commission & Church Committee in 70's found numerous abuses. CIA and FBI were mainly involved. Some examples:
  - CIA had exceeded authority collecting on US citizens
  - Illegal wiretaps
  - Administered LSD/radiation to unwitting US persons
  - Opened private mail/read private cables

Led To Intel Oversight Act of 1980 & EO 12333

Executive Order 12333

- Signed by President Reagan Dec, 1981
- Purpose: "... certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests."
- Regulates the collection of intelligence on US Persons or organizations.
- Applicable to all intelligence units and staff organizations that collect, analyze, process, retain, or disseminate intelligence information.
- Keep in mind that, "Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency."
- Not changed by USA Patriot Act of 2001

Key EO 12333 Implementing Regs in DoD

EO 12333: Collection only IAW implementing reg approved by AG

- **DOD Directive 5240.1 (*DOD Intelligence Activities*)**
- **DOD Directive 5240.1-R (*Procedures Governing the Activities of DoD Intelligence Components that Affect US persons*)**
- **SECNAV Instruction 3820.3D (*Oversight of Intelligence Activities within the Department o f the Navy)***
- **Army Regulation 381-10 (*U.S. Army Intelligence Activities)***
- **Air Force Instruction 14-104 (*Conduct of Intelligence Activities)***
- **Marine Corps Order 3800.2a (*Conduct and Oversight of Intelligence Activities)***

USA Patriot Act of 2001

"Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism" Act of 2001

- **Significant impact in permitting broad cooperation between IC & LE in the gathering and sharing of information related to terrorism.**
- **Impacts IO through various technical fixes to ECPA, Wiretap and Pen Register/Trap and Trace statutes. (see DoJ Field Guidance at** **http://www.cybercrime.gov/PatriotAct.htm)**
- **Other views of the Act's impact:**
  - ***How the USA-Patriot act puts the CIA back in the business of spying on Americans*** *Copyright* ***2001, The American Civil Liberties Union***
    http://www.aclu.org/congress/l102301j.html
  - ***TheUSA Patriot Act:*** *What's So Patriotic About Trampling on the Bill of Rights?*
    Copyright ***2001****, Center for Constitutional Rights*
    http://www.ccmep.org/hotnews/usapatriot1201.html
- **Intelligence oversight guidance remains *unchanged* by the legislation.**

USA Patriot Act -- Some Key Provisions Impacting IO

- Intelligence sharing w/ law enforcement expanded (sec 203/905)
  - Wholly new view of original 1947 intent /Post 9/11 example of need
  - 203a: Sharing of Grand Jury info re FI/CI with Federal Law Enforcement & Intelligence Community
  - 203b:Sharing wiretap info re FI/CI with Federal Law Enforcement & Intelligence Community *
  - 203c: AG required to establish procedures for 203a/b sharing (similar to DoDD 5240.1-R in response to EO12333)
  - 905: Requires AG to disclose to DCI any FI acquired by DoJ element during criminal investigation

•4 yr sunset (31 Dec 05)

Current CND Legal Issues

- **Tracing an Attack or Probe (Attribution)**
  - DoJ proposal for “global warrants”/ International cooperation
  - “Active Defense”/ “Computer Network Response” (Subterfuge for CNA?)
  - “Hack-back” (What’s this mean, anyway? Easy to violate laws.)

Spotting Legal Issues of Computer Network Defense

Who/What is the adversary?

- > Criminal? Terrorist? State? Combination?

Where is adversary located?

- > U.S.? International waters/airspace? Third Country? State of perpetrator?

What is impact on U.S.?

- > Minor disruptions ==> Damage to national security

Who should respond?

- > US? Host Country? Flag State?
- > U.S. Military? Law Enforcement?
- > Interagency Coordination?

Current CND Legal Issues (Cont)

- **Reading E-mail/Email Attachments to maintain OPSEC/Minimize**
  - - Concern of afloat CO's/Commanders real and legitimate
  - - SysAd Monitoring or COMSEC Monitoring?
  - Added issue of web based email
  - What about attachments to email under Minimize?
- **Scanning Wireless Networks Entry Points during Red Teaming Ops**
  - A Significant Threat
  - Hard for SA to know if installed
  - Scanner can pick up non-.mil IP's, but must read header info to determine
  - Wiretap Statute (18 USC 2511 (1)): Intentional Intercepts
  - Pen Register/Trap & Trace (18 USC 3121 (b)(2))

"Preparing the IO Battlefield"

- Collecting intelligence
  - –Non-intrusive (e.g., SIGINT)
  - –Intrusive, e.g.,
    - Assuring later access (e.g., trap doors)
    - Latent malicious logic plants
  - – Very Intrusive, e.g.,
    - Disrupt, Deny, Degrade or Destroy data or information

"Hey! They're lighting their arrows! . . . Can they DO that?"

THREAT ASSESSMENT

Russian Position ...

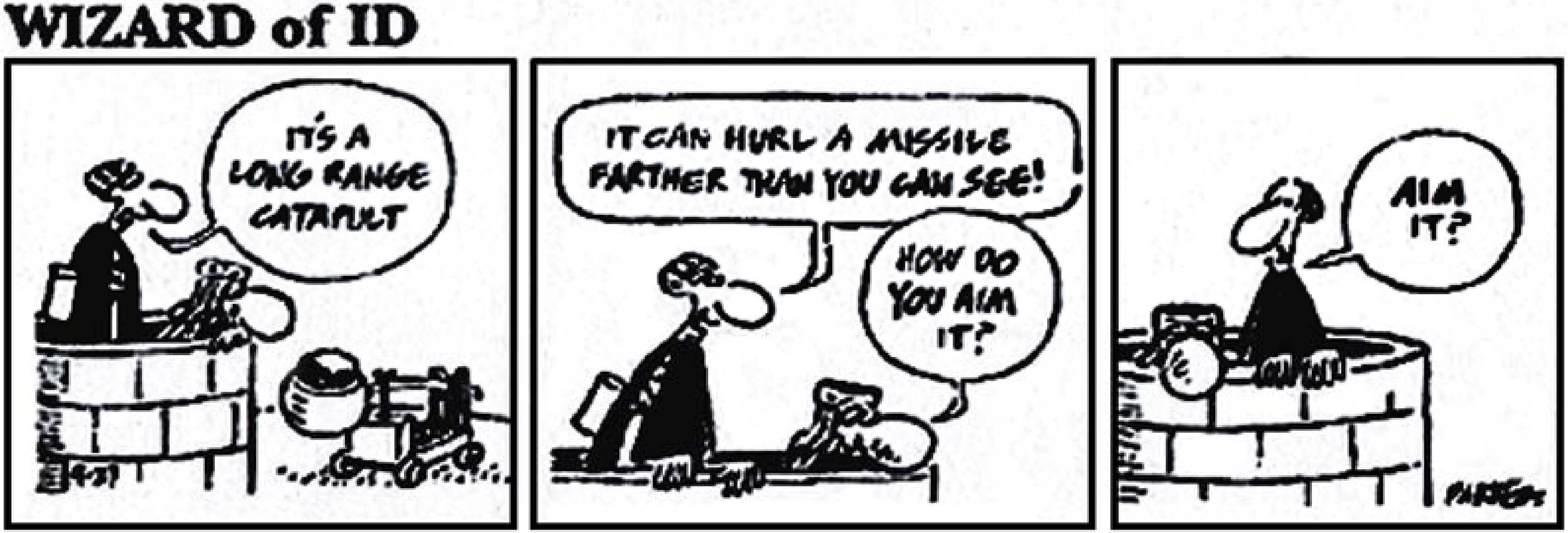
… The use of information warfare means will not be considered a non-military phase of a conflict, whether there are casualties or not. Considering the possible catastrophic consequences of strategic IW means by an enemy... Whether upon economic or state command and control systems, or on the combat potential of the armed forces ... *Russia retains the right to use nuclear weapons.*

Dr. V. I. Tsymbol - Speech at
Russian-U.S. Conference (1995)

Scenario - "Armed Attack"

- NYSE Computer is attacked by virus, destroying data. Effect on U.S. economy is serious, but not devastating. A hostile government claims responsibility and states that attacks will continue until sanctions imposed against it are lifted. Further attacks of this type will devastate U.S. economy. Intelligence agencies have identified the military facility in the hostile nation where the attacks are planned and executed
- Is the use of the virus an "armed attack?"
- May the U.S. respond with armed force? With a similar measure?
- What if no one claimed responsibility?

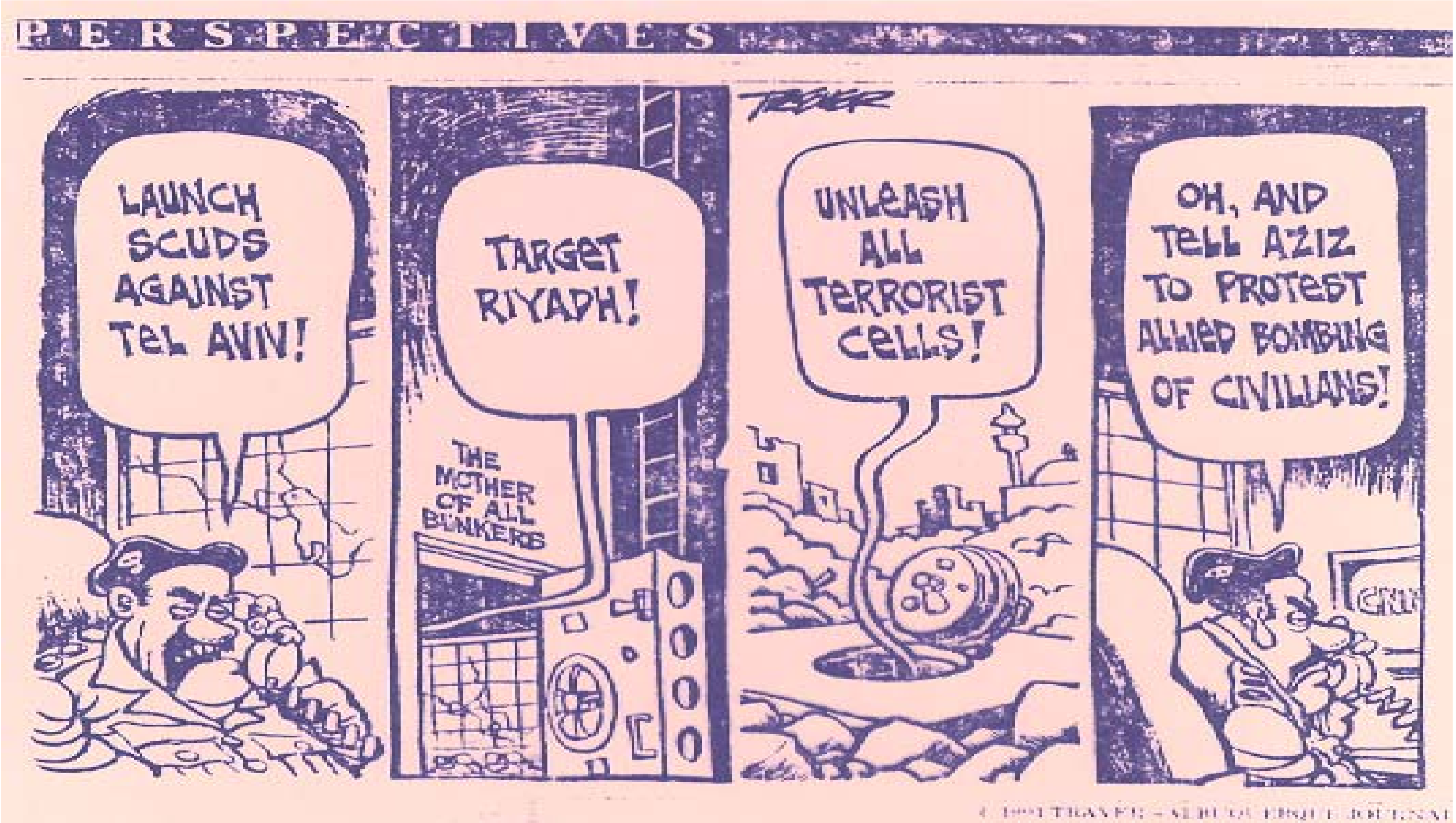
DISCRIMINATION


WIZARD of ID
IT'S A LONG RANGE CATAPULT
IT CAN HURL A MISSILE FARTHER THAN YOU CAN SEE!
HOW DO YOU AIM IT?
AIM IT?
PARKER

International Law & IO - Use of Force

- **UN Charter Art 2(4) prohibits "use of force against the territorial integrity ... of any state."**
  - **Two exceptions: Art 51 - use of force in self-defense IRT "armed attack"**
    Art 42 - use of force as authorized by the Security Council ("Chapter VII" enforcement operations).
- **What kinds of electronic attacks will be treated as a "use of force" under International Law?**
  - **HERF Guns?**
  - **CNE/CNA?**
- **Probable answer: International community will focus on consequences of attack, rather than the means used.**
  - **E.g., injury, death, property damage, release of dangerous forces, disruption of national security capabilities during crisis.**

DISTINCTION


PERSPECTIVES
LAUNCH SCUDS AGAINST TEL AVIV!
TARGET RIYADH!
THE MOTHER OF ALL BUNKERS
TREVER
UNLEASH ALL TERRORIST CELLS!
OH, AND TELL AZIZ TO PROTEST ALLIED BOMBING OF CIVILIANS!
CNN

© 1991 TREVER - ALBUQUERQUE JOURNAL

IO & Law of War: Distinction & Discrimination

- Distinction: Must distinguish combatants/lawful military targets from noncombatants/civilian objects
- Discrimination: IO Weapon/Tool must be discriminating, or capable of being controlled (i.e., can be directed at a military target).
- IO Issues:
  - Convergence of military and civilian infrastructures and information systems
  - Combatant acts may only be performed by combatants (i.e., uniformed military personnel). Can a civilian technician "pull the IO trigger?

IO & Law of War: Indiscriminate Weapons

- Must be able to direct weapons, once released, against lawful military targets
- Is the electron the "ultimate PGM?"
- IO related Issues:
  - Will IO effects of CNA tools spread beyond target systems? (E.g., malicious logic implants, viruses, worms, etc.)
  - Will IO activities cause dangerous unforeseen effects? (disease, fire, flood, radioactivity, etc.)

Law of Armed Conflict

1907 Hague Regulations: "The right of belligerents to adopt means of injuring the enemy is not unlimited."

- Necessity
- Proportionality
- Protected Persons and Places

Violation of Neutral's Rights

IO & Law of War: Necessity & Proportionality

- Commanders must consider incidental or collateral effects of attacks on health and safety of civilians and other noncombatants
  - Cannot be excessive in relation to anticipated military gain.
- Commanders must take reasonable steps to find out how civilians rely on infrastructure for health and safety
  - Targeting decision must first conduct proportionality balancing test for each target
- Intelligence, targeting, and command issues
  - Should ascertain the architecture of the target system to allow evaluation any associated or networked civilian systems, e.g., emergency services
  - Should consider the cascading effect a loss of a particular node or connection may have on the target infrastructure; e.g., would other redundant systems be overwhelmed and fail if the target system load was transferred

SUPERFLUOUS INJURY AND UNNECESSARY SUFFERING

BOUND & GAGGED
WE USE ONLY 100%
LOW-IN-SATURATED
FAT BOILING
OIL

IO & Law of War: Superfluous Injury

- Cannot use weapons that cause unnecessary death and suffering, or create wounds not treatable by traditional medical procedures.
- Russian report -- radiation and information can harm, even kill, computer operators
  - Virus "666" has reportedly killed 50
- Japanese Report -- a cartoon with flashing lights disturbed cognitive processes, and,
  - Changed behavior
  - Rendered viewers unconscious

IO & Law of War: Perfidy

- **Ruses are w/o question permissible in war, but some acts of deception (or dirty tricks) are prohibited.**
  - Without question, misuse of protection provided by law of war to obtain a combat advantage is prohibited, e.g., false use of electronic signals for hospitals, PW camps, medical aircraft and vessels
  - Perfidious acts such as feigning a truce or surrender, or feigning to be UN or neutral forces for purposes of attacking the enemy also prohibited.
  - Also, attacking while wearing the enemy's uniform is prohibited
- **IO provides much opportunity for ruses. Examples:**
  - Manipulating enemy visual, sensing, or other information systems so that enemy forces wrongly believe US troops are surrendering
  - Causing enemy to believe US combat vehicles are med vehicles or neutral vehicles. Same w/ manipulating enemy's targeting database so it believed a US HQ was a hospital is wrong.
  - Manipulating ID signals (e.g., squawking the enemy's IFF the so a nation's forces think approaching combat AC are actually friendly forces

IO & Law of War: Neutrality

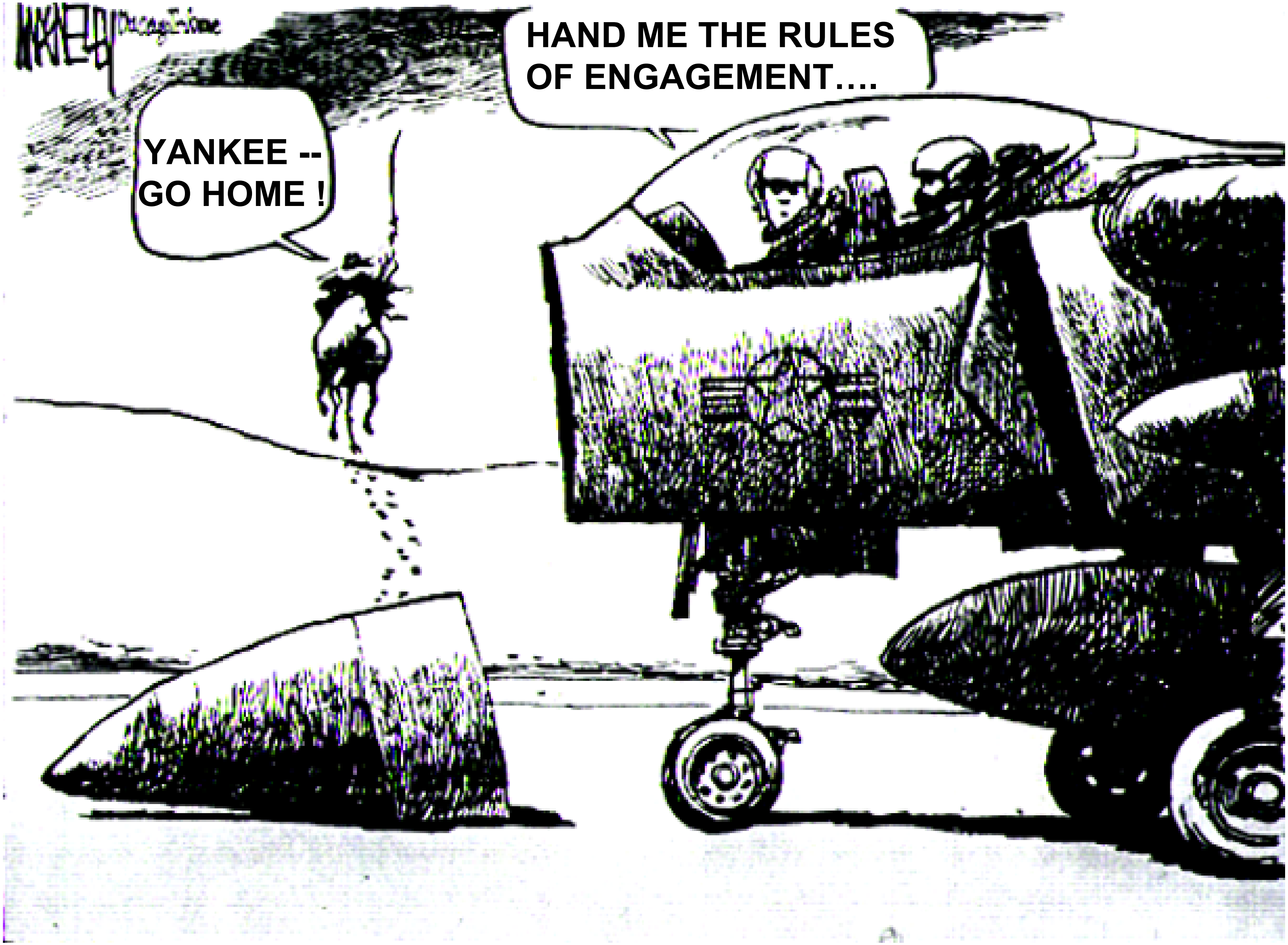
- Declared Neutrals are obligated not to provide militarily significant assistance to Belligerents
- Adversary may have a right of self-defense if a neutral assists a belligerent
- Issues for IO:
  - What information systems are militarily significant?
  - Treaty exception: communications relays (including satellites)
  - Satellite Systems run by international consortia

International Law & IO – Communications Treaties

- International Telecommunications Treaties Common Provisions:
  - General duty of non-interference
  - Partial exemption for military communications
  - National security and public safety exemptions, thus do not apply in armed conflict
- Generally, broadcasting from sea or aircraft with the intention of transmitting radio or television broadcasts into the territory of another State is prohibited

Assessment of IO & International Law Issues

- Should be able to apply the Law of Armed Conflict to IO with reasonable confidence. Less so with Use of Force applied to IO issues.
- Space & Communications: Primarily Treaty Issues, but Space issues need more consensus.
- Final Resolution of IO International Law issues may depend on the acts and statements of governments as events occur.
- U.S. needs to aggressively consider how it wants International Law to develop for IO.



HAND ME THE RULES OF ENGAGEMENT….
YANKEE -- GO HOME !

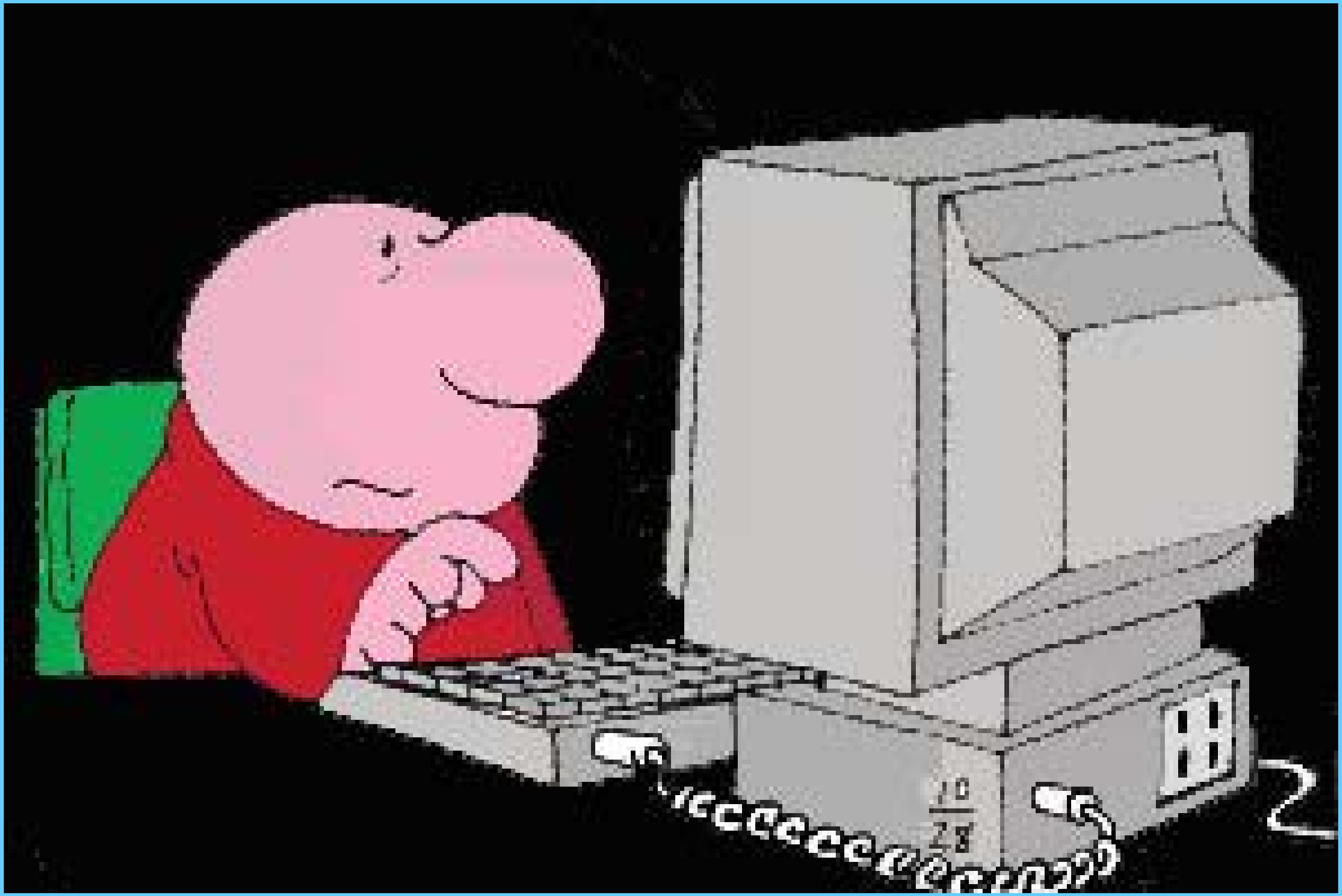
Lexington (19 April 1775))

"STAND YOUR GROUND MEN.
DON'T FIRE UNLESS FIRED UPON;
BUT IF THEY MEAN TO HAVE A WAR,
LET IT BEGIN HERE."

CAPT JONAS PARKER
to the Minutemen

IO and Rules of Engagement

- 2000 Revision to SROE
  - Enclosure F: “Information Operations (SECRET) - includes traditional elements, plus CNA and CND
  - Info Ops “Supplemental Measures”
- CNA/CND - Response to Hostile Act or Hostile Intent -- Attribution is the tough IO issue
- Bottom line - little agreement so little guidance
- As part of mission planning, ensure the IO cell has received clear guidance on what capabilities may be used, when, and under what circumstances.
- Similarly, ROE requests to use IO systems must be very specific to gain approval from higher authority.



… Now, let’s see if I can hack into the Base cafeteria files and order lobster for lunch …